# CISSP - Domain 1
## Security and Risk Management

*Writer: Viktor Nowiczenko*

### Confidentiality, Integrity and Availability

- Confidentiality - Strong Passwords, 2FA, Masking, Access Control, Least Privilege.
    - Data at rest - Encryption (ex. AES256)
    - Data in motion - Secure transport protocols (SSL, TLS, IPSEC)
    - Data in use - Physical locks and blocks, housekeeping
        - Threats: Social Engineering, Keyloggers, Cameras, IoT, Cryptanalysis

- Integrity - Protect against unauthorized data or system modifications
    - Cryptography, Check Sums, Hash (MD5, SHA1, SHA2), Access Control, Digital Signature
        - Threats: Code injection, Data alterations, Cryptanalysis

- Availability - Authorized people access data they need, when they need to.
    - IPS/IDS
    - Patch Management
    - Hardware redundancy: RAID, UPS, HVAC, staff, High Availability.
        - Threats: DDOS, System compromise, staff, application and hardware failure

### Disclosure, Alteration, and Destruction

- Disclosure
    - Someone unauthorized getting into your system/data.
- Alteration
    - Your data has been changed.
- Disclosure
    - Systems/Data rendered inaccessible.

## IAAA (Identification and Authentication, Authorization and Accountability):

- Identification
    - Name, username, ID number, employee number, Social Security Number etc.
- Authentication
    - Type I - Something you know: PIN, Passphrase etc.
    - Type II - Something you have: ID, Passport, token, cookie
    - Type III - Something you are: Biometrics, Fingerprint etc
- Authorization
    - Access Control
- Accountability
    - Auditing - Trace an action to a subject's identity: non-repudiation.

## Security Governance Principles

- Least Privilege – Minimum necessary access, no more.
- Need to Know - If you don't need to know, no access.
- Non-repudiation - Users can't deny having performed a certain action. Authentication + Integrity.
- Subject vs Object
    - Subject - Active users or program. Subjects manipulate objects.
    - Object - Passive data
- Governance vs Management
    - Governance
        - Balanced agreed upon objectives
        - Directions and decisions
        - Monitoring performance
        - Risk appetite management
    - Management
        - Plan, build and monitor activities in alignment with the directions
        - Practical work vs. Risk Appetite
- Organization and Management Structure
    - Top-Down: IT Leadership set the direction.
    - Bottom-Up: IT Security seen as a nuisance. Corrective actions

## Governance standards and control frameworks.

- PCI-DSS – Payment Card Industry Data Security Standard
    - Required standard for handling credit and debit cards
- OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation
    - Self directed risk management
- COBIT - Control Objectives for Information and related Technology.
    - Goals for IT – Stakeholder needs are mapped down to IT related goals.
- COSO - Committee of Sponsoring Organizations.
    - Goals for the entire organization.
- ITIL - Information Technology Infrastructure Library
    - IT Service Management (ITSM).
- FRAP - Facilitated Risk Analysis Process
    - Analyzes one business unit, application or system at a time in a roundtable brainstorm with internal employees. Impact analyzed, threats and risks prioritized.
- ISO 27000 series:
    - ISO 27001:  Establish, implement, control and improvement of the ISMS. Uses PDCA (Plan, Do, Check, Act)
    - ISO 27002: (From BS 7799, 1/2, ISO 17799) Provides practical advice on how to implement security controls. It has 10 domains it uses for ISMS (Information Security Management Systems).
    - ISO 27004: Provides metrics for measuring the success of your ISMS.
    - ISO 27005: Standards based approach to risk management.
    - ISO 27799: Directives on how to protect PHI (Protected Health
    - Information).

- Defence in Depth / Layered Defence / Onion Defence
    - Implemented multiple overlapping security controls to protect an asset.
    - Physical and Logical controls.
    - No single security control secures an asset.
    - Improves confidentiality, integrity and availability,

## Legal and Regulatory Issues

- Criminal Law
  - Proof must be “beyond reasonable doubt” and society is the victim
  - Incarceration, death and financial fines to punish and deter
- Civil Law
  - Financial fines compensate the victims
  - Must have ”the majority of proof” / Organizations, groups and individuals are the victims.
- Administrative Law
  - Laws enacted by government agencies (FDA Laws, HIPPA, FAA Laws)
- Private Regulations
  - Compliance is required by contract.
- Customary Law
  - Personal conduct and behavioural patterns founded in traditions of a region
- Religious Law
  - Based on religious beliefs in the area or country, include code of ethics and morals.

- Liability - Lack of Due Care would make management liable. ULTIMATELY - Senior Leadership
- Due Diligence *vs* Due Care:
  - Due Diligence – The research to build the IT Security architecture of your organization, best practices and common protection mechanisms, research of new systems before implementing.
  - Due Care - Prudent person care. Implementing the IT Security architecture, keep systems patched. If compromised: fix the issue, notify affected users (Follow the Security Policies to the letter)
  - Negligence - If a system under your control is compromised and you did ***NOT*** perform Due Care, you are most likely liable.
- Evidence
  - Real:  Physical and Tangible objects. USB Sticks, Hard Drive (Not Data)
  - Direct: Testimony from a 1st hand witness, their experience.
  - Circumstantial: Evidence to support for a point or other evidence.
  - Collaborative: Supporting facts or elements of a case.
  - Hearsay: Computer generated record. Not 1st-hand knowledge.
  -

    - ***Best Evidence:*** The courts prefer the best evidence possible. Evidence should be accurate, complete, relevant, authentic, and convincing.
    - ***Secondary Evidence*** – This is common in cases involving IT. Logs and documents from the systems are considered secondary evidence.
    - Evidence Integrity – Cannot be questioned.
        - Forensics are done on copies, never originals.
            - Check hash on both original and copy before and after forensics
    - Chain of custody: Who, When, What and Where handled the evidence.
- Reasonable Searches
    - Court determines if evidence was legally obtained
    - Employees must be aware they are monitored
    - 4th Amendment to US Constitution protects citizens from unlawful searches.
    - Exigent circumstances apply if there is an immediate threat to human life or evidence destruction.